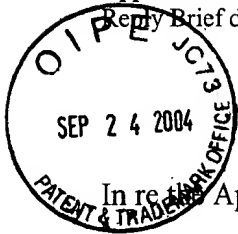


Appln. No.: 09/388,351

Reply Brief dated September 24, 2004



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Application of:

Erik J. SNAPPER, *et al.*

Serial No.: 09/388,351

Filed: September 1, 1999

For: System and Method for Populating
Forms with Previously Used Data
Values

Atty. Docket No.: 003797.77746

Group Art Unit: 2176

Examiner: William L. Bashore

Confirmation No.: 3809

REPLY BRIEF

Mail Stop: Appeal Brief-Patents
U.S. Patent and Trademark Office
220 20th Street S
Customer Window, Mail Stop Appeal Brief-Patents

RECEIVED

SEP 29 2004

Technology Center 2100

Sir:

This Reply Brief is submitted in accordance with 37 C.F.R. § 1.193 (b), filed in triplicate, in reply to the Examiner's Answer dated July 26, 2004. Please charge any necessary fees in connection with this Reply Brief to our Deposit Account No. 19-0733. Appellant's arguments begin on the following page.

ARGUMENT

The Examiner's Answer is largely repetitive of the arguments made by the examiner in the final Office Action dated November 28, 2003. The Examiner's Answer only specifically addresses four of Appellant's many arguments for patentability of the various pending claims, to which Appellant responds as set forth below.

Issue 1

Claims 3, 13-14, 21-22, 31, 40-41, 43, 46-47, and 50-54 stand rejected under § 103(a) as being unpatentable over Kikinis (U.S. Patent 5,794,259) in view of Light et al. (U.S. Patent 6,192,380) (hereinafter Light). This rejection is improper for the following reasons.

The examiner argues that the motivation to combine Kikinis with Light is the fact that they are allegedly in the same field of endeavor, i.e., filling in forms on Web pages. Examiner's Answer at 18-19. However, the mere fact that both references pertain to filling in forms on web pages does not lead to the conclusion that the references are in the same field of endeavor. Indeed, in an analogous case two references both regarding single in-line memory modules (SIMMs) were nevertheless determined to be in different fields of endeavor. *Wang Laboratories, Inc. v. Toshiba Corp.*, 993 F.2d 858 (Fed. Cir. 1993). While the examiner states which features of Kikinis and Light are being combined, the examiner provides no motivation or suggestion to combine the two references in the first place in order to solve the problem addressed by the claim. Examiner's Answer at 18. The only motivation to combine the references comes from Appellant's own specification, and the Federal Circuit has repeatedly stated that the limitations of a claim in a pending application cannot be used as a blueprint to

piece together prior art in hindsight, *In re Dembiczak*, 50 U.S.P.Q.2d 1614 (Fed. Cir. 1999). The Patent Office should rigorously apply the requirement that a teaching or motivation to combine prior art references needs to be provided. *Id.* The combination is thus the result of improper hindsight reasoning, and the rejection should be reversed.

Claims 4, 9, 10, 12, 15, 21, 26, 27, 28, 36, 37, 39, 42, 44

Claim 21 recites, *inter alia*, “comparing the field identifier of the selected field to previously stored field identifiers and, upon finding a match, displaying a list of suggested data values previously stored in response to one or more different forms previously filled in by the user...” The examiner argues that Kikinis’s bubble suggestions, e.g., illustrated in Kikinis, Fig. 2, teaches or at least suggests this claim element. Indeed, the examiner states that “analyzing/selecting the displayed bubble suggestion ... is analogous to analyzing/selecting its representative data value.” Examiner’s Answer at 19. However, regardless of the fact that the bubble suggestions of Kikinis have associated values, the user of a Kikinis system does not view or see what those associated values are prior to selection, and is left to guess which values will be inserted based on the selected tag. The presently claimed invention displays suggested data values (not tags or variables) so the user knows exactly what will be inserted into a form field. Contrary to the examiner’s allegation, selection of a specific data value and selection of a named group of data are not the same.

Claims 3, 22, and 31

Claim 3 recites, *inter alia*, “detecting a user-initiated action and inhibiting the copying of the suggested data value into the data entry region until after receipt of the user-initiated action.” The examiner argues that Kikinis teaches this claim limitation by stating “Kikinis produces a pop-up bubble of suggestions subsequent to an initial user action[.]. At this point Kikinis does not know what the user wants to choose, therefore, said bubble waits, and copying of data is inhibited, until Kikinis detects a selection (another user initiated action).” Examiner’s Answer at 20. However, the examiner is crediting Kikinis for disclosing something that is not there, namely, inhibiting copying. As previously argued, while Kikinis, at col. 3, lines 63-66, implies *waiting* for a user-initiated action prior to filling in the form, Kikinis does not actively *inhibit* activity prior to the user-initiation action, as is recited in the claim. The presently claimed invention addresses a security concern discovered as a result of previous inadequate solutions *such as is found in Kikinis*. Specifically, as discussed in the present application at p. 11, lines 9-22, and p. 13, lines 19-24, malicious web sites may attempt to execute a script which *mimics* user input. By mimicking user input, the malicious web site prompts systems such as Kikinis to fill in form fields and thus provide personal and/or confidential information (e.g., stored credit card numbers, passwords, etc.) to the malicious web site. It is specifically this security concern that the present invention addresses by actively *inhibiting* the copying of the suggested data value into the data entry region until after receipt of the user-initiated action, which is not taught or suggested by Kikinis.

Similarly, claims 22 and 31 recite, in pertinent part, “detecting a keystroke or mouse click from the user and inhibiting the copying of the suggested data value into the data entry region

until after receipt of the keystroke or mouse click.” Claims 22 and 31 are thus allowable for at least the same reason.

Claims 13 and 40

Claims 13 and 40 recite, in pertinent part, “detecting a password field and, upon detecting such a field, forcing the user to select whether a data value for that field will be stored for later use.” The examiner argues that, given the existence of HTML 4.0, it would have been obvious to implement masking of sensitive data. Examiner’s Answer at 20. Even if this were true, masking of sensitive data is not the same as forcing the user to select whether a data value for that field will be stored for later use, as recited in claims 13 and 40. Masking data as taught by HTML 4.0 involves displaying asterisks or other masking characters on a display screen in place of a user’s password as the user types in the password on a keyboard (or other input device). Thus the user’s password is not displayed for other people who might be in the same vicinity to see. Instead, anyone within view of the display screen on which the masking characters are displayed sees “*****” instead of the user’s actual password. On the other hand, the presently claimed invention forces the user to select whether a data value for a password field will be stored for later use. There is no masking required by the claim 13 or 40, and therefore HTML 4.0 is inapplicable. The rejection should be reversed.

In addition to the above, the examiner has not provided Applicants a reasonable opportunity to respond to the combination of Kikinis, Light, and “the existence of HTML 4.0.” That is, the examiner has not cited a specific reference that Applicants can analyze and comment on, and thus is an improper combination for a rejection under 35 U.S.C. § 103.

Claims 14 and 41

Claims 14 and 41 recite, *inter alia*, “performing numerical processing on the field to determine whether the field represents a credit card number and, in response thereto, suppressing suggestions.” The examiner argues that, given the existence of HTML 4.0, it would have been obvious to implement masking of sensitive data, Examiner’s Answer at 20, even though HTML 4.0 only masks passwords, not credit card numbers. Even if this were true, masking of sensitive data is not the same as performing numerical processing on the field to determine whether the field represents a credit card number and, in response thereto, suppressing suggestions, as recited in claims 14 and 41. Masking data as taught by HTML 4.0 involves displaying asterisks or other masking characters on a display screen in place of a user’s password as the user types in the password on a keyboard (or other input device). Thus the user’s password is not displayed for other people who might be in the same vicinity to see. Instead, anyone within view of the display screen on which the masking characters are displayed sees “*****” instead of the user’s actual password. On the other hand, the presently claimed invention performs numerical processing on the field to determine whether the field represents a credit card number and, in response thereto, suppresses suggestions so a user cannot access another user’s credit card number. There is no masking required by the claim 14 or 41, and therefore HTML 4.0 is inapplicable. The rejection should be reversed.

In addition to the above, the examiner has not provided Applicants a reasonable opportunity to respond to the combination of Kikinis, Light, and “the existence of HTML 4.0.”

That is, the examiner has not cited a specific reference that Applicants can analyze and comment on, and thus is an improper combination for a rejection under 35 U.S.C. § 103.

The examiner states that his answers also apply to Appellant's arguments with respect to the remaining claims. However, the examiner has failed to address distinct aspects of virtually every remaining claim other than those discussed above, as set forth below.

Claim 43

Claim 43 recites, *inter alia*, "detecting a password field and, upon detecting such a field, inhibiting the display of any suggested data values unless the Universal Resource Locator (URL) of the web site from which the form was generated matches a previously stored URL." The Examiner's Answer does not rebut Appellant's arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 54

Claim 54 recites, *inter alia*, "detecting that the one selected field is a password field and, in response thereto, determining whether the user has previously indicated whether a password should be stored for a URL on which the form resides and, if no such previous indication was made, prompting the user to indicate whether the password field should be stored for that URL." The Examiner's Answer does not rebut Appellant's arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claims 46, 50 and 52

Claims 46, 50 and 52 recite, *inter alia*, “detecting that the one selected field is a username field and, in response to the user selecting a suggested username, automatically copying a password previously used in response to the selected username into a separate password field on the web page.” The Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claims 47, 51 and 53

Claims 47, 51 and 53 recite, in pertinent part, “matching a URL associated with the form to a previously stored URL and, in response to a match failure, inhibiting the copying of the password.” The Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claims 6, 7, 24, 33, and 34

Claims 6, 24, 33 recite, in pertinent part:

comparing the field identifier of the selected field to a first plurality of dynamically updated historical identifiers previously extracted from a plurality of forms across a plurality of different web sites, and also to a statically created user profile comprising a second plurality of field identifiers having associated data values, and displaying suggested data values taken from both the historical identifiers and from the statically created user profile.

The Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claims 11, 38

Claims 11 and 38 recite, in pertinent part, “providing the user with an option to globally disable future storage of field data values.” The Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Issue 2

Claims 5, 23, and 32

Claims 5, 23, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kikinis in view of Light and further in view of Gupta et al. (U.S. Patent 6,199,079).

The examiner has not rebutted Appellant’s arguments that the combination of Kikinis, Light, and Gupta is improper, and has thus failed to provide a *prima facie* case of obviousness. Therefore, no further reply by Appellant is necessary.

Issue 3

Claims 8, 25, and 35

Claims 8, 25, and 35 each recite the use of a vCard schema. The Examiner’s Answer does not rebut Appellant’s arguments with respect to the use of a vCard schema, and thus no further reply by Appellant is necessary.

Issue 4

Claims 16-17, 19-20, 48-49, and 55 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Light et al. in view of Capps, U.S. Patent No. 5,666,502 to Capps.

The examiner has not rebutted Appellant's arguments that the combination of Light and Capps is improper, and thus all rejections under such combination should be reversed.

Claim 16, 19

Claim 16 recites, *inter alia*, "detecting that one of the text fields on the second form is correlated with one of the text fields on the first form despite having a different field identifier and, in response thereto, retrieving a corresponding previously stored data value from the local storage area." Claim 16 also recites, *inter alia*, "suggesting the data value retrieved in step (4) to the user as a possible value to be entered into the second form." The Examiner's Answer does not rebut Appellant's arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 17

Claims 17 recites, *inter alia*, "step (1) comprises the step of generating the first form from instructions retrieved from a first web site, and wherein step (3) comprises the step of generating the second form from instructions retrieved from a second web site." The Examiner's Answer does not rebut Appellant's arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 20

Claim 20 recites, in pertinent part, “inhibiting the release of the suggested data value until the user has manipulated a user input device.” Claim 20 is thus allowable for similar reasons as claim 3, discussed above. In addition, the Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 48

Claim 48 recites, similar to claim 50, “detecting that one of the text fields on the second form is a username field and, in response to the user selecting a suggested username, automatically copying a password previously used in response to the selected username into a separate password field on the second form.” Claim 48 is thus allowable for similar reasons as claim 50, discussed above. Furthermore, the Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 49

Claim 49 recites, similar to claim 51, “matching a URL associated with the second form to a previously stored URL and, in response to a match failure, inhibiting the copying of the password.” Claim 49 is thus allowable for similar reasons as claim 51, discussed above. Furthermore, the Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Claim 55

Claim 55 recites, similar to claim 54, “detecting that the one text field is a password field and, in response thereto, determining whether the user has previously indicated whether a password should be stored for a URL on which the form resides and, if no such previous indication was made, prompting the user to indicate whether the password field should be stored for that URL.” Claim 55 is thus allowable for similar reasons as claim 54, discussed above. Furthermore, the Examiner’s Answer does not rebut Appellant’s arguments with respect to these claim limitations, and thus no further reply by Appellant is necessary.

Issue 5

Claim 18

Claim 18 stands rejected under 35 U.S.C § 103(a) as unpatentable over Light et al. in view of Capps as applied to claim 16 above, and further in view of Applicants’ specification. The examiner has not rebutted Appellant’s arguments that the combinations of Light and Capps, and the combination of Light, Capps, and Applicant’s specification, are improper, and thus all rejections under such combinations should be reversed.

Claim 18 also adds the step of using Bayesian inference techniques. The Examiner’s Answer does not rebut Appellant’s arguments with respect to the use of Bayesian inference techniques, and thus no further reply by Appellant is necessary.

Issue 6

Claim 45

Claim 45 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Kikinis in view of Light et al. and further in view of Capps. The examiner has not rebutted Appellant's arguments that the combination of Kikinis, Light and Capps is improper, and thus all rejections under such combination should be reversed.

CONCLUSION

For all of the foregoing reasons, Appellants respectfully submit that the final rejections of claims 3-28 and 31-55 are improper and should be reversed.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: September 24, 2004

By:

A handwritten signature in black ink, appearing to read "Ross A. Dannenberg", is written over a horizontal line.

Ross A. Dannenberg
Registration No. 49,024
1001 G Street, N.W.
Washington, D.C. 20001-4597
Tel: (202) 824-3000
Fax: (202) 824-3001